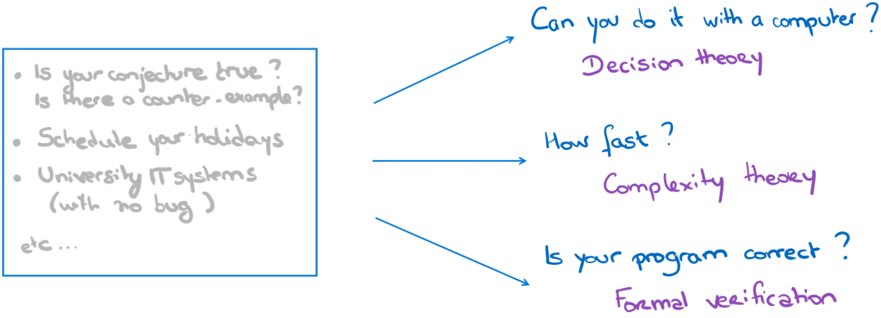
Something about semigroups in computer science

Laure Daviaud
University of East Anglia

You've got a problem...



Formal verification

How to get a program to check that another program is correct...?

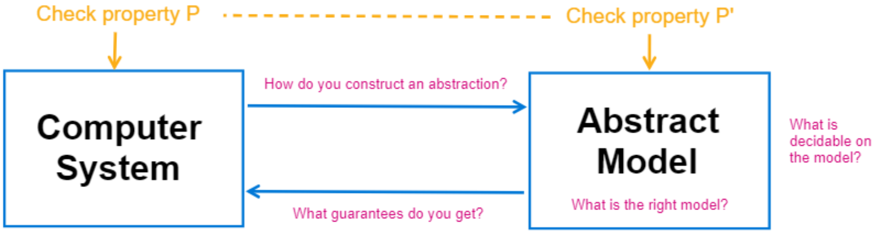
Using formal methods, mathematical abstractions...

If you have got one thing to remember...

$\longrightarrow$ Undecidable (unsurprinsingly)

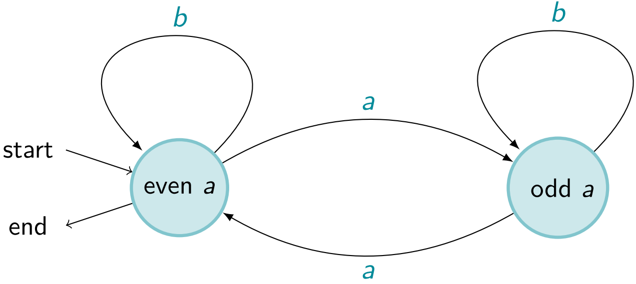
Though still worth trying to get some partial guarantee...

Formal verification



Automata

$\Sigma = \{a, b\}$



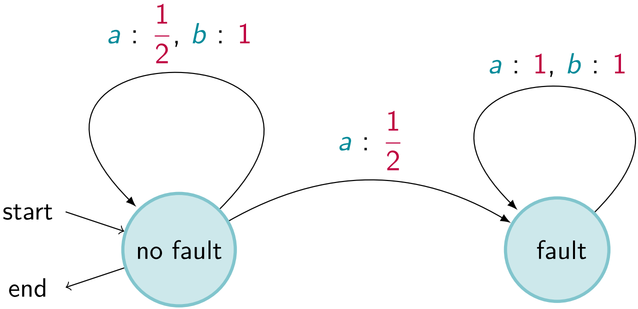
Accepts the language of words of Σ^* with an even number of a's

This is a semigroup!!

To take away:
Rational languages - everything is decidable, but simple model

Probabilistic Automata

$\Sigma = \{a, b\}$

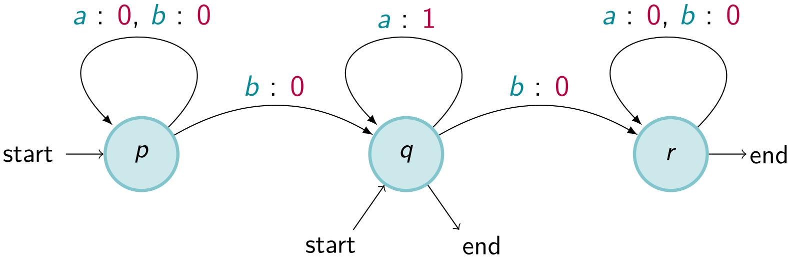


Maps a word of Σ^* with the probability of it not being faulty

This is also a semigroup!!

Max-plus Automata

$\Sigma = \{a, b\}$



What is computed on *aaabbaabbbaaaaabaa*?

Maps a word of Σ^* with its maximal number of consecutive a's

This is also a semigroup!!

The natural questions...

Consider:

A model computing a function from Σ^* to $\mathbb{R}$ (say)

Questions:

Are two models computing the same functions?
Are they approximatively computing the same function?
Is one always smaller than the other one?
etc...

Decidability varies a lot, depending on the question and on the model.

One question on one model

The Model

Max-Plus Automata

Extension of Boolean automaton with non-negative integers on transitions, combined using operations max and sum.

$$\Sigma^* \to \mathbb{N} \cup \{-\infty\}$$

The Question

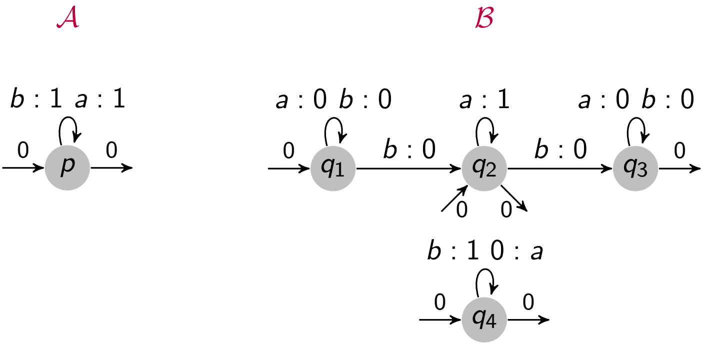
Big-O Problem

Given two max-plus automata computing functions f and g, is f big-O of g?

There exists C such that for all $w \in \Sigma^*$, $f(w) \leq Cg(w) + C$

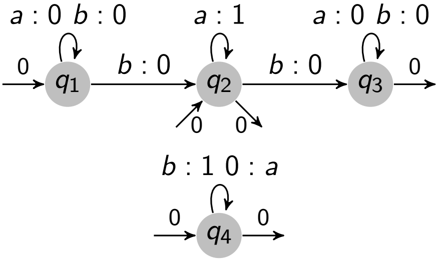
Theorem (D., Purser): It is decidable (PSPACE-complete).

Our running example



$\mathcal{B}$: $w \mapsto$ max of number of b's and number of consecutive a's in w

And matrices...

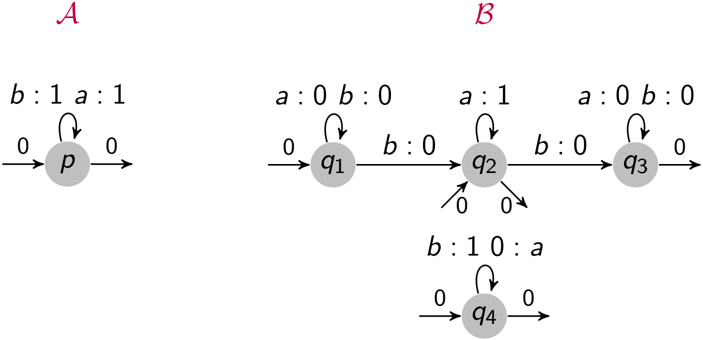


$$M(a) = \begin{pmatrix} 0 & - & - & - \\ - & 1 & - & - \\ - & - & 0 & - \\ - & - & - & 0 \end{pmatrix}$$

$$M(b) = \begin{pmatrix} 0 & 0 & - & - \\ - & - & 0 & - \\ - & - & 0 & - \\ - & - & - & 1 \end{pmatrix}$$

with $(I)_{q_1} = (I)_{q_2} = (I)_{q_4} = (F)_{q_2} = (F)_{q_3} = (F)_{q_4} = 0$

Witnesses



Key sequence: $(a^n b)^n a^n$

$$\left(n^2, \begin{pmatrix} 0 & n & n & - \\ - & - & n & - \\ - & - & 0 & - \\ - & - & - & n \end{pmatrix} \right)$$

Witnesses

$$\left(n^2, \begin{pmatrix} 0 & n & n & - \\ - & - & n & - \\ - & - & 0 & - \\ - & - & - & n \end{pmatrix} \right)$$

Becomes:

$$\left(\infty, \begin{pmatrix} 0 & 1 & 1 & - \\ - & - & 1 & - \\ - & - & 0 & - \\ - & - & - & 1 \end{pmatrix} \right)$$

- $-$: no run at all
- 0: all runs have weight 0
- 1: some runs with positive weights but not the largest growth rate
- ∞: runs with largest growth rate

Game plan

Aim: Decide some property P on an abstract model M

$\longrightarrow$ Find the right finite algebraic structure S to represent M

$\longrightarrow$ Find the right operations on S to capture P (no more, no less)

$\longrightarrow$ Identify witnesses, present in S if and only if M satisfies P

Running example

$$a = (p, 1, p, \begin{pmatrix} 0 & \text{-} & \text{-} & \text{-} \\ \text{-} & 1 & \text{-} & \text{-} \\ \text{-} & \text{-} & 0 & \text{-} \\ \text{-} & \text{-} & \text{-} & 0 \end{pmatrix}) \text{ and } b = (p, 1, p, \begin{pmatrix} 0 & 0 & \text{-} & \text{-} \\ \text{-} & \text{-} & 0 & \text{-} \\ \text{-} & \text{-} & 0 & \text{-} \\ \text{-} & \text{-} & \text{-} & 1 \end{pmatrix})$$

$$ab = (p, 1, p, \begin{pmatrix} 0 & 0 & \text{-} & \text{-} \\ \text{-} & \text{-} & 1 & \text{-} \\ \text{-} & \text{-} & 0 & \text{-} \\ \text{-} & \text{-} & \text{-} & 1 \end{pmatrix}) \quad bb = (p, 1, p, \begin{pmatrix} 0 & 0 & 0 & \text{-} \\ \text{-} & \text{-} & 0 & \text{-} \\ \text{-} & \text{-} & 0 & \text{-} \\ \text{-} & \text{-} & \text{-} & 1 \end{pmatrix})$$

Running example

$\longrightarrow$ Sharp

$$a^{\#} = (p, \infty, p, \begin{pmatrix} 0 & - & - & - \\ - & \infty & - & - \\ - & - & 0 & - \\ - & - & - & 0 \end{pmatrix}) \quad a^{\#}b = (p, \infty, p, \begin{pmatrix} 0 & 0 & - & - \\ - & - & \infty & - \\ - & - & 0 & - \\ - & - & - & 1 \end{pmatrix})$$

$$a^{\#}ba^{\#}b = (p, \infty, p, \begin{pmatrix} 0 & 0 & \infty & - \\ - & - & \infty & - \\ - & - & 0 & - \\ - & - & - & 1 \end{pmatrix})$$

$$(a^{\#}ba^{\#}b)^{\#} = (p, \infty, p, \begin{pmatrix} 0 & 0 & \infty & - \\ - & - & \infty & - \\ - & - & 0 & - \\ - & - & - & \infty \end{pmatrix})$$

Running example

$\longrightarrow$ Flat

$$(a^{\#}ba^{\#}b)^{\flat} = (p, \infty, p, \begin{pmatrix} 0 & 0 & 1 & \text{-} \\ \text{-} & \text{-} & 1 & \text{-} \\ \text{-} & \text{-} & 0 & \text{-} \\ \text{-} & \text{-} & \text{-} & 1 \end{pmatrix})$$

Game plan

Aim: Decide whether $\mathcal{A}$ big-O of $\mathcal{B}$

$\longrightarrow$ Find the right finite algebraic structure S to represent M

$\longrightarrow$ Find the right operations on S to capture P (no more, no less)

$(p, \overline{x_a}, q, \overline{M(a)})$ closed under product, sharp and flat

$\longrightarrow$ Identify witnesses, present in S if and only if M satisfies P

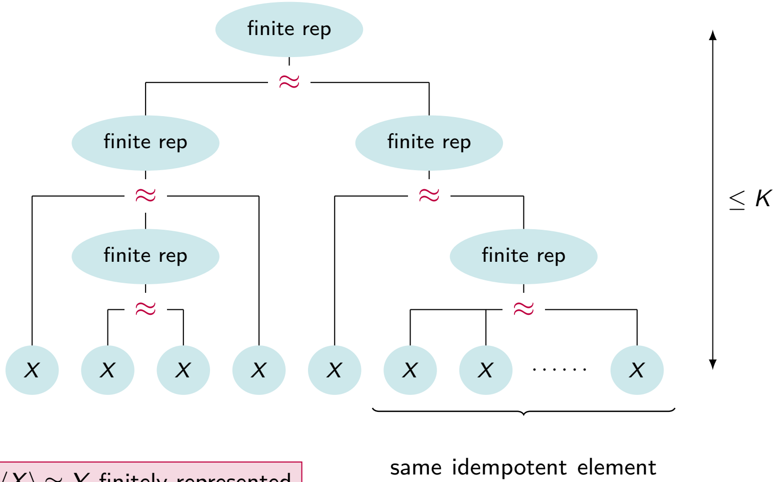
$$(p, x, q, M)$$

with:

- p initial, q final
- $x = \infty$
- $IMF \neq \infty$

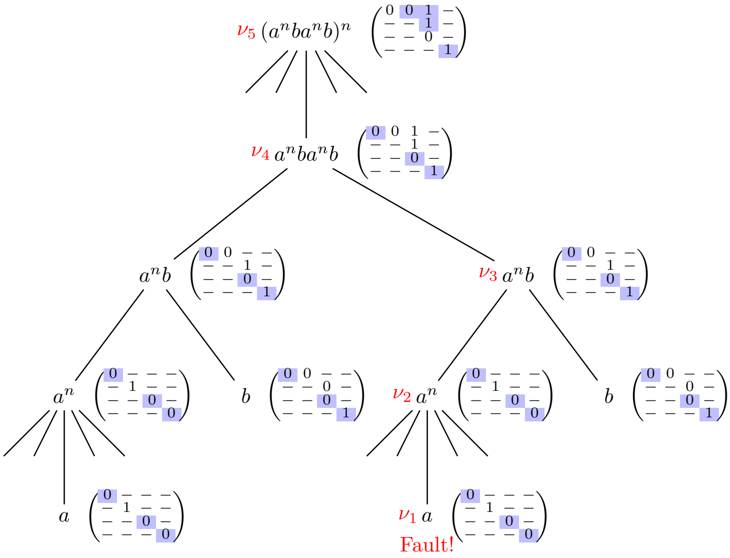
The factorisation forest theorem of Simon

In any finite semigroup...



$\langle X \rangle \approx Y$ finitely represented

Just a fancy picture



The End (or just the beginning)

Theorem [D., Purser]

The big-O problem is PSPACE-complete for max-plus automata.

Proposition [D., Purser, Tcheng]

Construction of witnesses with increasing complexity.